REMARKS

The Applicant and the undersigned thank Examiner Nalven and SPE Morse for their careful review of this application and especially for their time and consideration given during the telephonic interview of February 9, 2004. A summary of this telephonic interview is provided below.

Claims 1-57 have been rejected by the Examiner. Upon entry of this amendment, Claims 2, 5, 15, 41, and 51 have been cancelled while Claims 1, 3-4, 6-14, 16-40, 42-50, and 52-57 remain pending in this application. The independent claims are Claims 1, 14, 25, 37, 50, and 56.

Consideration of the present application is respectfully requested in light of the above claim amendments to the application, the telephonic interview, and in view of the following remarks.

Summary of Telephonic Interview of February 9, 2005

The Applicant and the undersigned thank Examiner Nalven and SPE Morse for their time and consideration given during the telephonic interview of February 9, 2005. During this telephonic interview, a proposed amendment to the claims was discussed. The Applicant provided the proposed amendment to the claims in advance of the interview on February 4, 2005.

The Applicant's representative explained that the invention as recited in the amended independent claims detects data signatures at a communications layer that is different from that of U.S. Patent No. 6,301,668 issued in the name of Gleichauf et al. (hereinafter, the "Gleichauf reference"). It was explained that the Applicant's technology monitors communications for data signatures at the application layer (known to those of ordinary skill in the art as layer "seven" in the open systems interconnection data communications model) while the Gleichauf reference monitors communications at the network and transport layers (known to those of ordinary skill in the art as layers "three" and "four" in the open systems interconnection data communications model).

The Applicant's representative further explained that none of the prior art of record, such as the Geleichauf reference, provides any teaching of monitoring communications for data signatures at the application layer in combination with evaluating context information related to the data signature where the context information comprises one of an application layer data field

type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature.

As an example, it was explained that the invention as recited in the amended independent claims can search for data signatures by looking for a text string and determining if the text string is listed as a subject line in an e-mail or if it is used in a command line to execute a file. The Applicant's representative noted that this example is discussed in the originally filed application on pages 15-16, and specifically, paragraphs [0042-0043].

Meanwhile, the prior art, such as the Gleichauf reference, monitors communications at an entirely different communications layer compared to the claimed invention such as the network and transport layers. The Gleichauf reference monitors communications at these levels to evaluate protocols in manner that is different from the claimed invention, as will be discussed in more detail below. The Gleichauf reference does not look for data signatures and the Gleichauf reference does not look for any context of data signatures as recited in the amended independent claims.

After listening to the Applicant's representative's discussion of the amended claims, Examiner Nalven and SPE Morse stated that these amendments would be considered when a formal response is submitted and that an update search would need to be conducted by Examiner Nalven.

The Applicant and the undersigned request Examiner Nalven to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.

Claim Rejections Under 35 U.S.C. §§ 102 and 103

The Examiner rejected Claims 1-6, 14-15, 18-21, 25-26, 32, 34, 37-42, 50-51, and 54-56 under 35 U.S.C. § 102(e) as being anticipated by the Gleichauf reference. The Examiner rejected Claims 7-8, 10-12, 22, 27, 29-31, 43-44, 46-48, and 57 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of U.S. Pat. No. 5,991,881 issued in the name of Conklin et al. (hereinafter, the "Conklin reference").

The Examiner rejected Claims 9, 23, and 45 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Conklin reference, and further in view of U.S. Patent Application Publication No. 2002/0083331, published in the name of Krumel

(hereinafter, the "Krumel reference"). The Examiner rejected Claims 13 and 49 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Conklin reference, and further in view of a Printed Publication entitled, "Detecting Backdoors," authored by Zhang et al. (hereinafter, the "Zhang reference").

The Examiner rejected Claims 16, 35, and 52 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of U.S. Patent No. 6,301,668 issued in the name of Ji et al. (hereinafter, the "Ji reference"). The Examiner rejected Claims 17 and 53 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Ji reference, and further in view of a Printed Publication entitled, "Security Reality Check," authored by Farrow (hereinafter, the "Farrow reference").

The Examiner rejected Claim 24 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Conklin reference, the Krumel reference, and further in view of the Zhang reference. The Examiner rejected Claim 28 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Conklin reference, and further in view of the U.S. Patent No. 6,275,942 issued in the name of Bernhard et al (hereinafter, the "Bernhard reference"). The Examiner rejected Claims 33 and 36 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Krumel reference.

The Applicant respectfully offers remarks to traverse these pending rejections. The Applicant will address each independent claim separately as the Applicant believes that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) detecting a data signature by evaluating communications at an application layer level between a target and a suspect; (2) correlating said data signature with an application layer fingerprint of the target to determine to what extent said target is vulnerable to said data signature; (3) evaluating contextual information related to the data signature to determine a likelihood that said target is under attack, the contextual information comprising at least one of (4) an application layer data field type used

to encapsulate the data signature and (5) an application layer protocol type used to transmit the data signature, as recited in amended independent Claim 1.

The Gleichauf Reference

The Gleichauf reference generally describes a system for adaptive network security using network vulnerability assessment. The network environment can comprise devices that form an internal network, protection for the internal network, and an external network. The internal network, indicated generally at 10, can comprise a plurality of workstations 12 coupled to a network backbone 14. Network backbone 14 can comprise, for example, an Ethernet, FDDI, token ring, or other type of network backbone. Protection for internal network 10 can be provided by firewall 16 and a router 18 which are coupled to network backbone 14. Router 18 serves as a gateway between internal network 10 and an external network 30. External network 30 can be, for example, the Internet or other public network. Firewall 16 can serve to limit external access to resources in internal network 10 and protect these internal resources from unauthorized use. See Figure 2 of the Gleichauf reference reproduced below, and in column 4, lines 40-58.

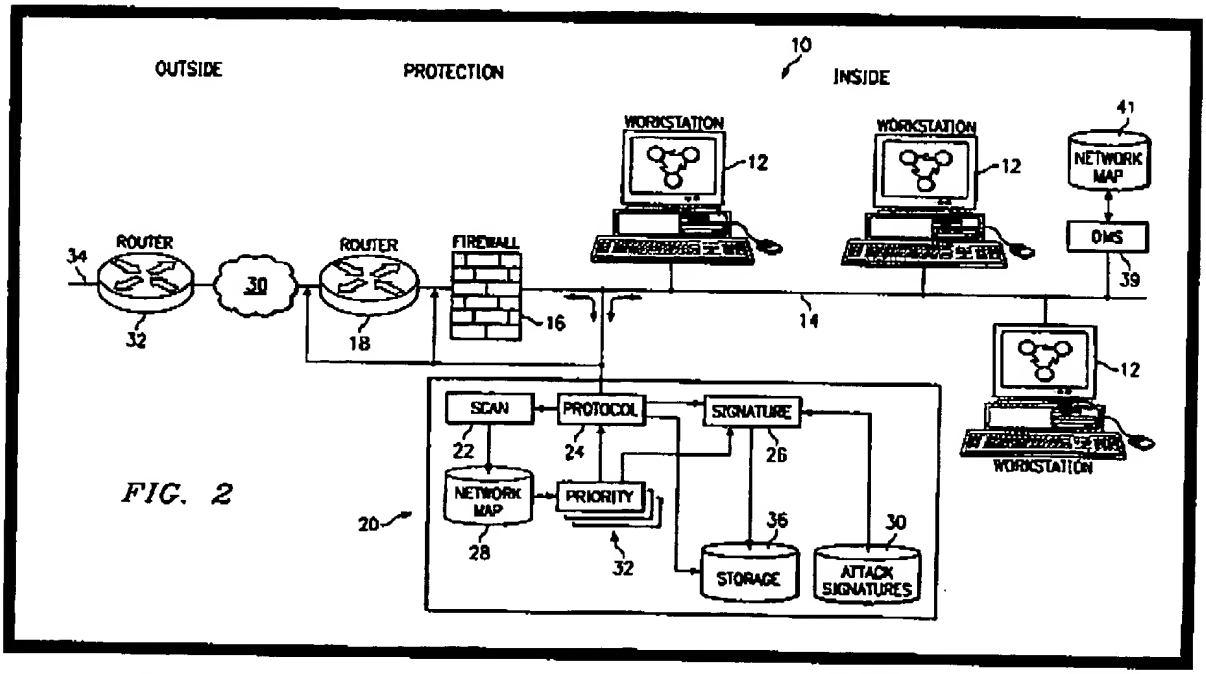


FIG. 2

Internal network 10 of the Gleichauf reference further comprises a network security system 20 coupled to network backbone 14. The network security system 20 can include a scan

engine 22 and a protocol engine 24 coupled to network backbone 14. A signature engine 26 is coupled to protocol engine 24. The scan engine 22 is further coupled to network map 28. The signature engine 26 is coupled to attack signatures 30. A priority engine 32 is coupled to network map 28, protocol engine 24 and signature engine 26. The protocol engine 24 and signature engine 26 are each also coupled to a storage 36. See the Gleichauf reference, column 4, lines 58-68.

The Gleichauf reference explains that the protocol engine 24 performs a plurality of protocol analyses upon monitored traffic on network backbone 14 in order to detect attacks upon the network. Attacks upon the network include unauthorized accesses, policy violations, and patterns of misuse. The protocol engine 24 can perform the following protocol analyses upon monitored traffic on network backbone 14: checksum verification (IP, TCP, UDP, ICMP, etc.), IP fragment reassembly, TCP stream reassembly, protocol verification (such as insuring the IP header length is correct and the TCP data gram is not truncated), and timeout calculations. See the Gleichauf reference, column 6, lines 24-37.

The signature engine 26 of the Gleichauf reference is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signatures 30. Attack signatures 30 can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. Signature engine 26 can compare packets from the network traffic with such attack signatures 30 such that policy violations can be discovered. See the Gleichauf reference, column 6, lines 38-45.

The Gleichauf Reference Does Not Use Contextual Information

Opposite to the protocol engine 24 and signature engine 26 of the Gleichauf reference, the invention described by amended independent Claim 1 monitors communications at an applications layer instead of the network and transport layers. Further, the invention as recited in amended independent Claim 1 evaluates data signatures in combination with contextual information related to data signatures. The contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature.

The Gleichauf reference evaluates protocols separately from its data signatures. That is, the Gleichauf reference uses a protocol engine 24 to evaluate protocol information separately from a signature engine 26. The Gleichauf signature engine 26 only monitors network level communications traffic for text that matches certain signatures.

The Conklin Reference

The Examiner admits that the Gleichauf reference fails to teach listening for a response to a data signature from a target. To make up for this deficiency, the Examiner relies upon the Conklin reference.

The Conklin reference describes systematic monitoring, intrusion identification, notification, and tracking of unauthorized activities, such as methods or systems used by "hackers" to intrude computer networks. The Conklin reference teaches a star configuration of two Ethernet network segments 'B' and 'C' and a terminal network connection leading to a network surveillance device for a computer network as illustrated in Figure 2. The system of the Conklin reference broadcasts communications between any two computers on an Ethernet segment that is monitored by an out-of-line surveillance device. See Conklin reference, column 2, lines 58-66.

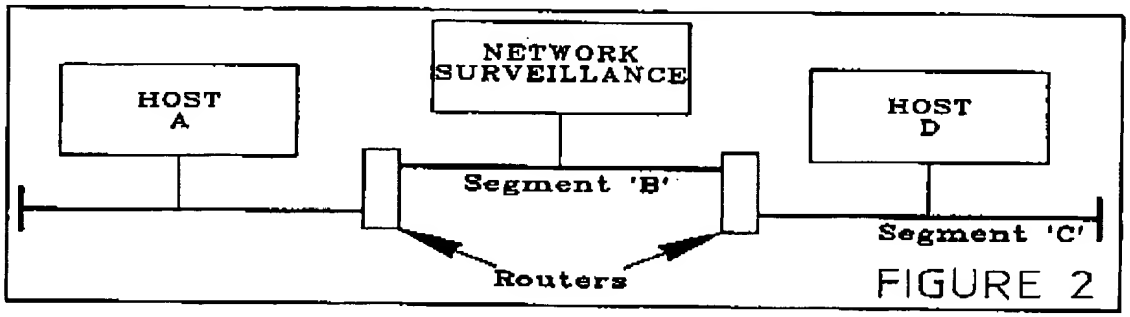


FIGURE 2

The Conklin reference explains that its intrusion detection may incorporate algorithms or patterns to detect attempted intrusions or intrusions on the network. As each packet of network data is passed from the network observation function, the intrusion detection function examines the data in comparison to a series of predefined or learned patterns which are pre-stored or developed from data received from the network.

In the Conklin reference, the network data is compared to a database of known patterns. If the collected data matches the databases stored data, individually or collectively, then the network surveillance system identifies the network data as a reportable activity and the network

surveillance system components are activated and a data channel is opened between the network observation function and the evidence logging function.

Similar to the Gleifchauf reference, the Conklin reference does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Conklin reference, like the Gleichauf reference, only evaluates data signatures alone without any context.

The Krumel Reference

The Examiner admits that the Gleichauf reference fails to teach determining if a packet is an unknown command. To make up for this deficiency, the Examiner relies upon the Krumel reference.

The Krumel reference has a data protection system 1 that is coupled through a port to router 2 (or cable modem or other preferably broadband, persistent network connection access device), which is linked through a broadband connection to other computer systems and networks, exemplified by Internet 8 and Internet Service Provider (ISP) 10. Packets of data are transmitted from an ISP, such as ISP 10, via Internet 8 to router 2. The packets are transmitted to data protection system 1, which analyzes the packets in "real time" and without buffering of the packets, while at the same time beginning the process of transmitting the packet to the internal network(s) in compliance with the timing requirements imposed by the Ethernet or other network standards and protocols. See Figure 1 of the Krumel reference reproduced below.

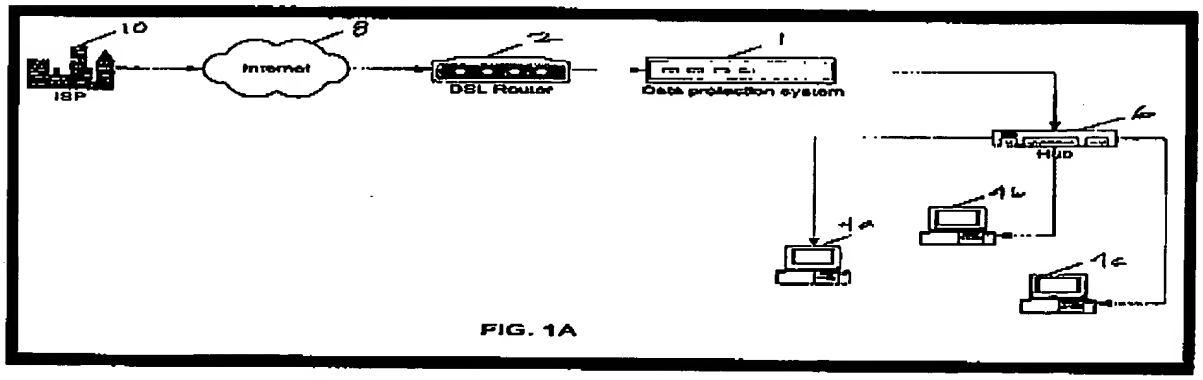


FIG. 1A

If a packet of data in the Krumel system satisfies the criteria of the rules-based filtering performed within data protection system 1, which is executed in a manner to be completed by the time the entire packet has been received by data protection system 1, then it is allowed to pass to hub 6 as a valid packet, which may then relay the cleared packet to computers 4a, 4b, 4c, etc. on the internal network. If a packet of data fails to meet the filtering criteria, then it is not allowed to pass as a valid packet and is "junked." Without the intermediate positioning of data protection system 1, the packets would be transmitted directly to unprotected hub 6, thereby exposing computers 4a, 4b and 4c to security risks. Similar filtering is performed on packets that are to be transmitted from computers 4a, 4b, and 4c to Internet 8. See the Krumel reference, page 4, paragraphs [0067-0068].

The Krumel reference explains how TCP (transmission control protocol) and UDP (user datagram protocol) packets are evaluated in parallel where TCP and UDP are host-to-host protocols located in the transport layer of the protocol stack. See Krumel reference, page 8, paragraph [0092].

Meanwhile, opposite to the Krumel reference, the invention as recited in amended independent Claim 1 evaluates data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Krumel reference, like the Gleichauf reference, only evaluates data signatures alone without any context.

The Zhang Reference

The Examiner admits that the Gleichauf and Conklin references fail to teach suspicious behavior comprising the transmitting of a root shell prompt to a suspect node. To make up for this deficiency, the Examiner relies upon the Zhang reference.

The Zhang reference generally describes protocol specific algorithms that look for signatures particular based on different protocols. Specifically, the Zhang reference describes algorithms that find "backdoors" in a flood of legitimate network traffic. See Section 6. - Summary of the Zhang reference.

The Zhang reference does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where

the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Zhang reference, like the Gleichauf reference, only evaluates data signatures alone without any context.

The Applicant also notes that the Zhang reference may not constitute enabling prior art because of its high-level description or lack of enabling detail for its algorithms. But even if the Zhang reference was enabling prior art, it still would not teach evaluating data signatures at an applications layer in combination with contextual information related to data signatures as recited in amended independent Claim 1.

The Ji Reference

The Examiner admits that the Gleichauf reference fails to teach a protocol comprising HTTP protcol. To make up for this deficiency, the Examiner relies upon the Ji reference.

The Ji reference describes a corporate environment 202 that includes a host computer 204 and host computer 206, which are connected to a proxy server 208, representing in this example an HTTP proxy server that is interposed between the distributed computer network 112 (such as the internet) and the host computers of corporate environment 202. The host computer 204 represents any computer that is capable of requesting and receiving data transfers from distributed computer network 112 and may be implemented using any of the suitable operating systems such as Windows. See Figure 2 of the Ji reference reproduced below.

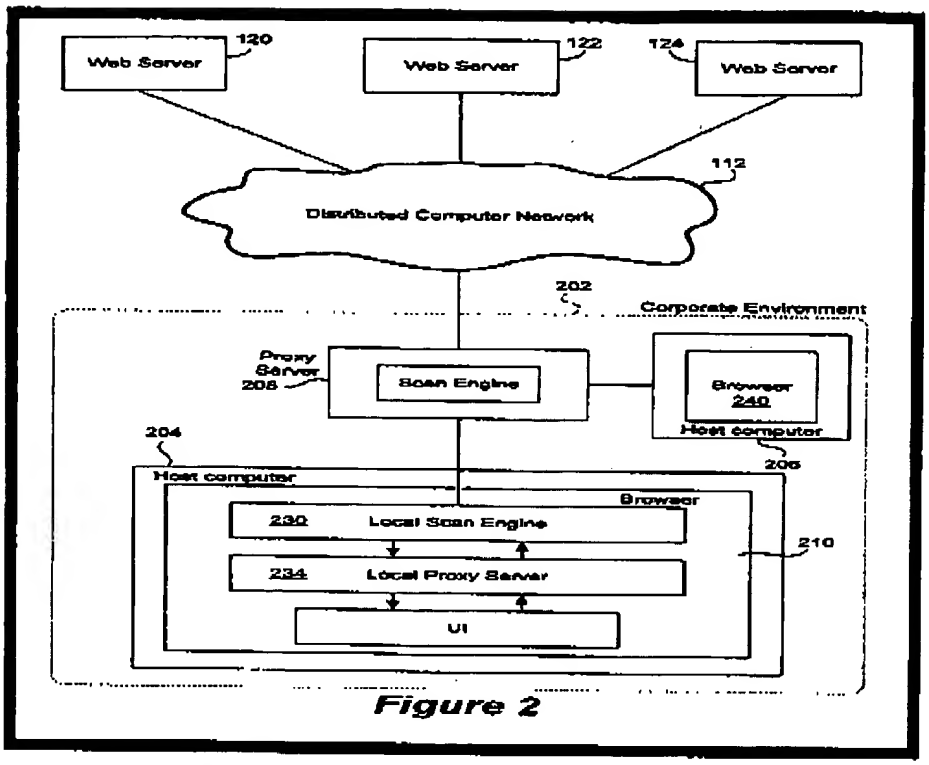


Figure 2

The host computer 204 of the Ji system may access distributed computer network 112 via a commercial browser such as Internet Explorer by Microsoft Corporation. The browser 210 within host computer 204 is set to request an auto-config script, i.e., a set of codes that automatically starts upon the occurrence of some predefined event, from proxy server 208 when browser 210 is started up. See the Ji reference, column 5, lines 21-56.

With the auto-config script, a distributed virus scanning module or engine at each host computer 204 is preferably created and/or updated each time a new browser threat is activated and/or an initial HTTP request is issued therefrom. The distributed virus scan engine at each host computer 204 can be created from codes/data centrally maintained at one or more servers. The distributed virus scan engine preferably employs the information contained in virus definition files maintained at one or more servers on the LAN in order to perform its own virus scan at its host computer. In this manner, the advantages associated with centrally managed virus scanning solutions (e.g., ease of maintenance and updates as there are fewer servers involved) are achieved while the disadvantages (e.g., periodic manual updating and maintenance at each host computer) are avoided. See the Ji reference, column 5, lines 5-20.

The Ji reference, like the Gleichauf reference, does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Ji reference, like the Gleichauf reference, only evaluates data signatures alone without any context.

The Farrow Reference

The Examiner admits that the Gleichauf and Ji references fail to teach detecting a data signature of "cgi-bin/phf." To make up for this deficiency, the Examiner relies upon the Farrow reference.

The Farrow reference is a product review article that describes various intrusion detection systems that were available in July 1999. The Farrow reference mentions the "cgi-bin/phf" string in a section of the article that addresses stealth attacks. The authors of the article tested several IDS products with this string.

The Farrow reference, like the Gleichauf reference, does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Farrow reference, like the Gleichauf reference, only evaluates data signatures alone without any context.

The Applicant also notes that the Farrow reference may not constitute enabling prior art because of its high-level description of products in the market during July 1999. But even if the Farrow reference was enabling prior art, it still would not teach evaluating data signatures at an applications layer in combination with contextual information related to data signatures as recited in amended independent Claim 1.

The Bernhard Reference

The Examiner admits that the Gleichauf and Conklin references fail to teach the data signature being a passwd in a context where filenames are likely to appear To make up for this deficiency, the Examiner relies upon the Bernhard reference.

The Bernhard reference describes a computer network 100 that includes a second line firewall 106 connected to a LAN server 112. The computer network 100 also includes a third firewall 108, a Kerberos server 110, an intranet Web server 114, a plurality of data processing systems (i.e., workstations) 116a-n, and an Internet Web server 118. All of these network elements connected to LAN 101 are monitored for computer misuse using an intrusion detection system (IDS) software 120. See Figure 1 of the Bernhard reference blow.

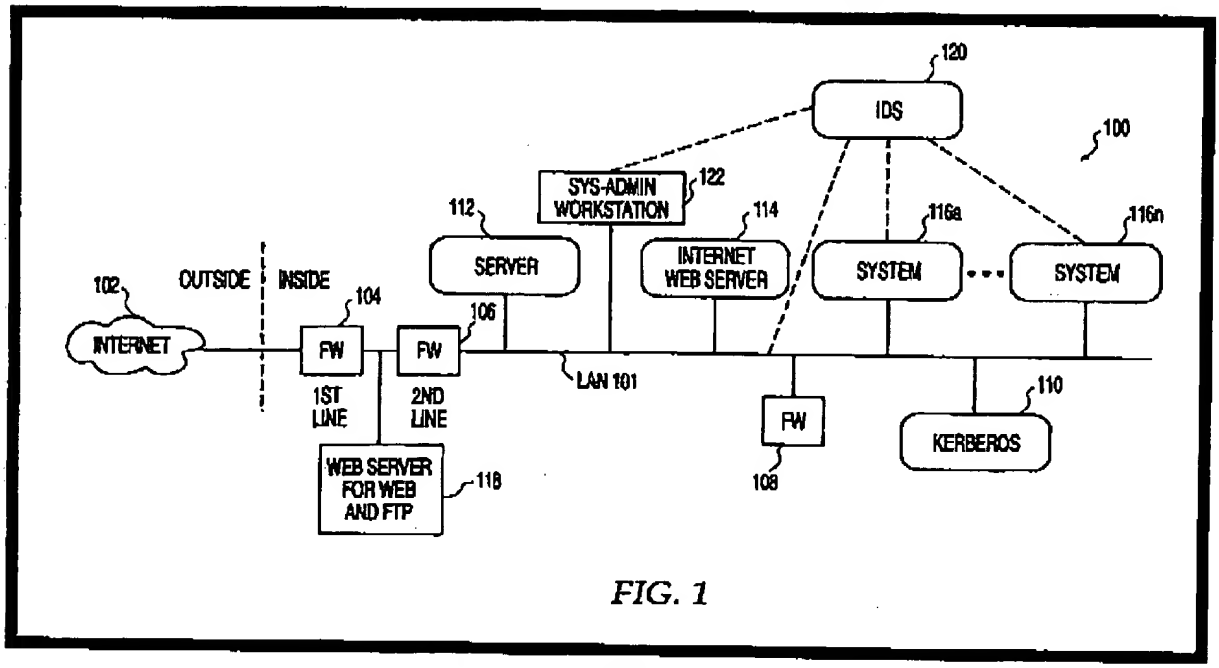


FIG. 1

The IDS software 120 of the Bernhard reference may reside and be centrally configured and monitored from a sysadmin workstation 122. The IDS software 120, as indicated in FIG. 1, may also reside on one or more of the network elements (e.g., data processing systems 116) as well as at various points within the LAN 101 between network elements (thereby acting as network-level detectors). The IDS software 120 may operate on any number of principles, such as the one specified in U.S. Pat. No. 5,557,742 issued to Smaha et al. The ARMs of the Bernhard reference operate with the particular misuse engine of the IDS software 120 selected and installed by the sysadmin of the computer network 100 in a "plug and play" manner. In

other words, the ARMs reside in the IDS software 120. See the Bernhard reference, column 5, lines 1-25

The Bernhard reference explains that its product provides for automatic response to computer system misuse using active response modules (ARMs). The Bernhard reference describes steps of defining a plurality of ARMs to process instances of computer misuse, receiving an instance of misuse from an intrusion detection system (the instance of the misuse having been detected by the misuse engine) and identifying ARMs associated with and activated for the detected computer misuse. The method then, for each of the identified ARMs, collects pertinent data from the misuse engine and invokes each of the identified ARMs with the pertinent data. See the Bernhard reference, column 4, lines 26-39.

As noted above, the Bernhard reference describes what actions are taken after a security event is detected. The Bernhard reference does not relate or describe how security events are detected as evidenced above by the admission that the IDS software 120 may operate on any number of principles, such as the one specified in U.S. Pat. No. 5,557,742 issued to Smaha et al. It follows that the Bernard reference, like the Gleichauf reference, does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature.

Conclusion Regarding Independent Claim 1

In light of the differences between Claim 1 and the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection of Claim 1 are respectfully requested.

Independent Claim 14

The rejection of Claim 14 is respectfully traversed. It is respectfully submitted that the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a data

signature encapsulated in an application layer data field and directed at a target using an application layer protocol; (2) evaluating a context of the data signature context by one of: (3) reviewing the application layer data field type or (4) reviewing the application layer protocol type; and (5) determining whether the data signature poses a threat based on said context of said data signature, as recited in amended independent Claim 14.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of a data signature context by one of: reviewing the application layer data field type and reviewing the application layer protocol type, as recited in amended independent Claim 14.

In light of the differences between Claim 14 and the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 14. Accordingly, reconsideration and withdrawal of this rejection of Claim 14 are respectfully requested.

Independent Claim 25

The rejection of Claim 25 is respectfully traversed. It is respectfully submitted that the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) monitoring a plurality of data transmissions at an applications layer level between a suspect and a target to identify one or more data signatures, (2) the data transmissions indicating a current state of communication between the suspect and the target; (3) evaluating contextual information related to each data signature, the contextual information comprising at least one of (4) an application layer data field type used to encapsulate a respective data signature and (5) an application layer protocol type used to transmit a respective data signature; and (6) evaluating a likelihood that the target is under attack based on the contextual information of one or more data signatures of transmissions and a current state of communication, as recited in amended independent Claim 25.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating contextual information related to each data signature, the contextual information comprising at least one of an application layer data field type used to encapsulate a respective data signature and an application layer protocol type used

to transmit a respective data signature; and evaluating a likelihood that the target is under attack based on the contextual information of one or more data signatures of transmissions and a current state of communication, as recited in amended independent Claim 25.

In light of the differences between Claim 25 and the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 25. Accordingly, reconsideration and withdrawal of this rejection of Claim 25 are respectfully requested.

Independent Claim 37

The rejection of Claim 37 is respectfully traversed. It is respectfully submitted that the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) detecting a data signature by evaluating communications at an application layer level between a target and a suspect; (2) correlating said data signature with a fingerprint of the target to determine to what extent said target is vulnerable to the data signature; and (3) evaluating contextual information related to the data signature to determine a likelihood that the target is under attack, the contextual information comprising at least one of (4) an application layer data field type used to encapsulate the data signature and (5) an application layer protocol type used to transmit the data signature, as recited in amended independent Claim 37.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating contextual information related to the data signature to determine a likelihood that the target is under attack, the contextual information comprising at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature, as recited in amended independent Claim 37.

In light of the differences between Claim 37 and the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 37. Accordingly, reconsideration and withdrawal of this rejection of Claim 37 are respectfully requested.

Independent Claim 50

The rejection of Claim 50 is respectfully traversed. It is respectfully submitted that the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a data signature encapsulated in an application layer data field directed at a target using an application layer protocol; (2) evaluating said a context of the data signature by one of: (3) reviewing the application layer data field type; (4) reviewing the application layer protocol type; and (5) determining whether the data signature poses a threat based on said context of said data signature, as recited in amended independent Claim 50.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of the data signature by one of: reviewing the application layer data field type and reviewing the application layer protocol type, as recited in amended independent Claim 50.

In light of the differences between Claim 50 and the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 50. Accordingly, reconsideration and withdrawal of this rejection of Claim 50 are respectfully requested.

Independent Claim 56

The rejection of Claim 56 is respectfully traversed. It is respectfully submitted that the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) monitoring a plurality of data transmissions at an applications layer level between a suspect and a target to identify one or more data signatures, the data transmissions indicating a current state of communication between said suspect and said target; (2) evaluating contextual information related to each data signature, the contextual information comprising at least one of (3) an application layer data field type used to encapsulate a respective data signature and (4) an application layer protocol type used to transmit a respective data signature; and (5) evaluating a likelihood that the target is under attack based on the contextual information of one or more data signatures of said transmissions and said current state of communication, as recited in amended independent Claim 56.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating contextual information related to each data signature, the contextual information comprising at least one of an application layer data field type used to encapsulate a respective data signature and an application layer protocol type used to transmit a respective data signature, as recited in amended independent Claim 56.

In light of the differences between Claim 56 and the Gleichauf, Conklin, Krumel, Zhang, Ji, Farrow, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 56. Accordingly, reconsideration and withdrawal of this rejection of Claim 56 are respectfully requested.

Dependent Claims 3-4, 6-13, 16-24, 26-36, 38-40, 42-49, 51-55, and 57

The Applicant respectfully submits that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicant also respectfully submits that the recitations of these dependent claims are of patentable significance.

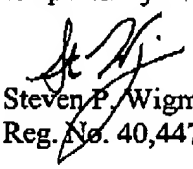
In view of the foregoing, the Applicant respectfully requests that the Examiner withdraw the pending rejections of dependent Claims 3-4, 6-13, 16-24, 26-36, 38-40, 42-49, 51-55, and 57.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on November 5, 2004. The Applicant and the undersigned thank Examiner Nalven for consideration of these remarks. The Applicant has amended the claims and has submitted remarks to traverse rejections of Claims 1-57. The Applicant respectfully submits that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, please contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,



Steven P. Wigmore
Reg. No. 40,447

March 7, 2005
King & Spalding LLP
191 Peachtree Street, N.E.
Atlanta, Georgia 30303-1763
telephone: (404) 572.4600
K&S File No. 05456-105035